PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-217890
(43)Date of publication of application : 02.08.2002

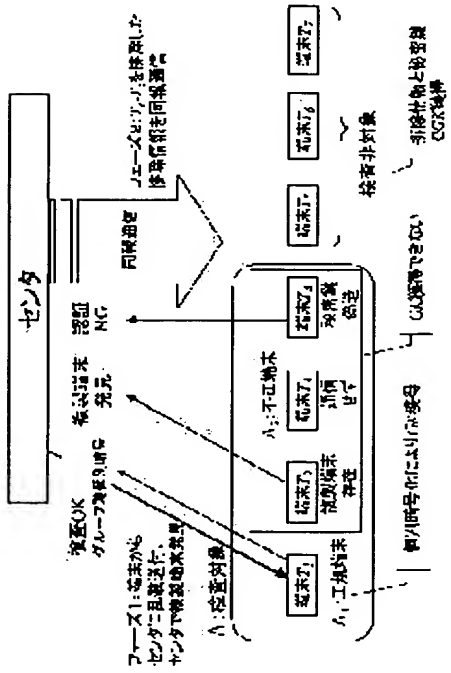
(51)Int.Cl. H04L 9/08
G09C 1/00
H04L 9/32

(21)Application number : 2001-013250
(22)Date of filing : 22.01.2001

(71)Applicant : ADVANCED MOBILE TELECOMMUNICATIONS SECURITY TECHNOLOGY RESEARCH LAB CO LTD
(72)Inventor : MATSUZAKI NATSUME
ANZAI JUN
MATSUMOTO TSUTOMU

(54) METHOD OF FINDING REPLICATED TERMINAL

(57)Abstract:
PROBLEM TO BE SOLVED: To automatically find and exclude a replicated terminal in a communication system consisting of a center and a plurality of terminals.
SOLUTION: The center and a plurality of the terminal are connected through a communication network for ciphering communication with individual group keys. The center sends challenge information, in the case of delivering a new group key to the terminals. Each of the terminals sends response information obtained by ciphering terminal ID and a terminal random number to a center public key to the center, which retrieves a communication log to inspect the presence/absence of terminals, having the same terminal ID and different terminal random numbers. If there are corresponding terminals, it is determined that the replicated terminal exists, and the session key is not delivered. Since random number generated by an original terminal is difficult to replicate, the replicated terminal cannot generate the same random number, so that the existence of the replicated terminal can be detected. When the replicated terminal is found, the multi-address communication of exclusion information that this has been excluded is performed, to deliver the same group keys to unchecked terminals.



LEGAL STATUS

[Date of request for examination] 26.03.2001
[Date of sending the examiner's decision of rejection] 05.04.2005
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－217890
（P2002－217890A）
(43)公開日　平成14年８月２日(2002.8.2)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ　9/08		Ｃ０９Ｃ　1/00	６４０Ｂ	５Ｊ１０４
Ｇ０９Ｃ　1/00	６４０	Ｈ０４Ｌ　9/00	６０１Ｂ	
Ｈ０４Ｌ　9/32			６０１Ａ	
			６０１Ｅ	
			６７５Ｂ	

審査請求　有　請求項の数23　ＯＬ　（全 18 頁）

(21)出願番号　特願2001－13250(P2001－13250)

(22)出願日　平成13年１月22日(2001.1.22)

(71)出願人　597174182
株式会社高度移動通信セキュリティ技術研究所
神奈川県横浜市港北区新横浜三丁目20番地８

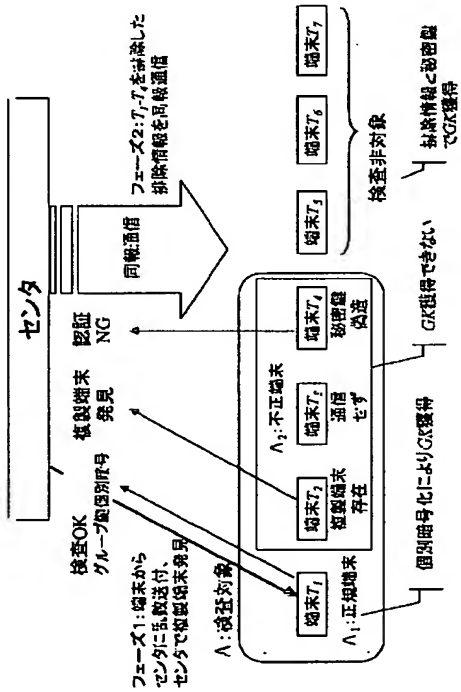
(72)発明者　松崎　なつめ
神奈川県横浜市港北区新横浜三丁目20番８号　株式会社高度移動通信セキュリティ技術研究所内

(74)代理人　100099254
弁理士　役　昌明　（外１名）

最終頁に続く

(54)【発明の名称】　複製端末発見方法

(57)【要約】
【課題】　センタと複数台の端末からなる通信システムにおいて、複製端末を自動的に発見して排除する。
【解決手段】　センタと複数台の端末は、個々のグループ鍵で暗号通信する通信網により接続されている。センタは、端末に新規グループ鍵を配布する際に、チャレンジ情報を送る。端末は、端末IDと端末乱数をセンタ公開鍵で暗号化したレスポンス情報をセンタに送る。センタは、通信ログを検索して、同一端末IDで端末乱数の異なる端末の有無を検査する。該当する端末があれば、複製端末が存在すると判断して、グループ鍵を配布しない。オリジナル端末で発生した乱数は複製困難であり、複製端末は同じ乱数を発生できないので、複製端末の存在を検出できる。複製端末が発見されたとき、これを排除した排除情報を同報通信することにより、未チェックの端末に同じグループ鍵を配布する。



【特許請求の範囲】

【請求項１】　センタＣと複数台の端末T_i（ｉは端末ＩＤ）を含むグループ同報通信システムの複製端末発見方法において、

前記センタＣは、センタ乱数Z^b（上付きｂはラウンド番号を示す添字）を生成し、グループ鍵の更新通知と前記センタ乱数Z^bをチャレンジＣＨＡとして同報通信を用いて前記複数台の端末に送信し、

前記チャレンジＣＨＡを受信した端末T_iは、ラウンドｂにおける端末乱数$R_i{}^b$を生成し、前記センタ乱数Z^bと前記端末乱数R^bに対する端末認証文$D_i{}^b$を端末秘密鍵S_iにより生成し、前記端末認証文$D_i{}^b$と前記端末乱数$R_i{}^b$とをセンタ公開鍵Ｙｃで暗号化して端末暗号文$E_i{}^b$として前記センタＣに送信し、

前記センタＣは、グループ鍵ＧＫを生成し、センタ秘密鍵Ｓｃで前記端末暗号文$E_i{}^b$を復号して前記端末認証文$D_i{}^b$と前記端末乱数$R_i{}^b$とを得て、端末公開鍵Y_i（センタが端末秘密鍵を管理している場合は端末秘密鍵S_i）で前記端末認証文$D_i{}^b$を検証し、前記端末乱数$R_i{}^b$と、前記端末T_iの端末ＩＤとを、対応させて登録したデータベースを検索して、同一端末ＩＤでかつ異なる端末乱数が登録されている重複登録の有無を検査し、前記端末認証文$D_i{}^b$の検証結果が正しく、かつ前記重複登録が無い前記端末T_i（正規端末と称する）の前記端末乱数$R_i{}^b$と前記端末ＩＤを前記データベースに登録し、この正規端末の端末乱数$R_i{}^b$を用いて、前記グループ鍵ＧＫを暗号化してセンタ暗号文$EC_i{}^b$として前記正規端末T_iに送信し、前記端末認証文$D_i{}^b$の検証結果が正しくないか、前記重複登録がある端末T_i（不正端末と称する）とすでに前記グループ鍵ＧＫを暗号化して送信した前記正規端末とを排除して前記グループ鍵を共有するための排除情報を求めて、前記排除情報を同報通信で送信し、

前記正規端末T_iは、前記センタ暗号文$EC_i{}^b$を受信し、前記端末乱数$R_i{}^b$を用いてこれを復号して前記グループ鍵ＧＫを得て、前記正規端末と前記不正端末以外のその他端末の端末T_iは、前記センタＣから前記排除情報を受信し、前記端末T_iの秘密鍵S_iを用いて前記グループ鍵ＧＫを得て、

前記不正端末T_iは、前記センタ暗号文$EC_i{}^b$あるいは排除情報を用いても、前記グループ鍵ＧＫを得ることができずにグループ同報通信から排除されることを特徴とする複製端末発見方法。

【請求項２】　センタＣは、前記その他の端末に、現用グループ鍵を必要条件とするグループ鍵情報を配布し、前記その他の端末は、現用のグループ鍵と配布されたグループ鍵情報とを使って新しいグループ鍵を得ることを特徴とする請求項１記載の複製端末発見方法。

【請求項３】　前記端末は、センタＣが発生し送信するチャレンジＣＨＡの代わりに、前記端末乱数をもとにして端末認証子を生成し、前記センタＣは、前記チャレンジＣＨＡの生成と送信をしないことを特徴とする請求項１記載の複製端末発見方法。

【請求項４】　前記ｎ台の端末からｄ台を選択してサブグループを形成し、前記センタＣは、前記認証文D_iの検証結果が正しく、かつ前記データベース検出がない端末T_iの集合（正規端末集合）Λ1と、前記D_iの検出結果が正しくない、あるいは前記データベース検出された端末T_iの集合（不正端末集合）Λ2に、サブグループ内の端末を分別し、前記集合Λ1の各端末T_iからの乱数R_iを用いて前記グループ鍵を暗号化して前記センタ暗号文EC_iを求めて、前記サブグループに含まれる端末を排除してグループ鍵を共有するための排除情報を求めて、以上の暗号文と排除情報を全端末に同報通信を用いて送信することを特徴とする請求項１記載の複製端末発見方法。

【請求項５】　センタＣと個別の識別子を保持するｎ台の端末（ｎは２以上の整数）からなり、センタが指定した端末を除いてグループ鍵を配送可能な同報通信システムにおいて、

秘密鍵をＳとし、前記秘密鍵Ｓと前記台数ｎより大きい素数または素数のべき数をｐとし、（ｐ－１）の約数をｑとし、特定端末数をｄ（$1 \leq d < n-1$）とし、前記各端末T_i（$1 \leq i \leq n$）は、$d \leq k-2 < n$を満たすｋを決定し、

$S = \Sigma \lambda(i, \Lambda) \times S_i$（和はｉ∈Λについて行なう）

（ただし、

$S_i = S + f_1 \times i + \cdots + f_{k-1} \times i^{k-1} \bmod q$

（$f_1, \cdots, f_{k-1}$は（ｋ－１）個のＧＦ(ｑ)の元、ただし、$f_{k-1} \neq 0$）

$\lambda(i, \Lambda) = \Pi\{L/(L-i)\}$（積はＬ∈Λ－{ｉ}について行なう）

Λは、前記ｎ台の端末およびダミーから選んだ任意のｋ台からなる集合）を満たす個別の秘密鍵S_iを秘密に保持しており、前記センタＣは、さらに（ｋ－１）個のダミーの秘密鍵を、

$S_{n+1} = S + f_1 \times (n+1) + \cdots + f_{k-1} \times (n+1)^{k-1} \bmod q$，・・・，

$S_{n+k-1} = S + f_1 \times (n+k-1) + \cdots + f_{k-1} \times (n+k-1)^{k-1} \bmod q$

により計算して、各ｉ（$1 \leq i \leq n+k-1$）について

$Y_i = g \hat{} S_i$　（ＧＦ(ｐ)上の演算）

とし、

$Y = g \hat{} S$　（ＧＦ(ｐ)上の演算）

としたとき、前記センタＣは、前記（Ｓ，ｐ，ｑ，ｇ，Ｙ，$Y_1, \cdots, Y_{n+k-1}$）を保持し、前記端末T_iは、前記（S_i，ｐ，ｑ）を保持し、前記センタは、前記すでに前記グループ鍵ＧＫを暗号化して送信した端末と、前記端末認証文の検証結果が正しくない、あるいは前記データベースに重複登録がある合計ｄ台の特定端末$T_{i1}, \cdots,$

T_{id}を排除するために、（１）零でないＧＦ(q)の元ｒを求めて、準備情報
$C1=g^r$　（ＧＦ(p)上の演算）
を計算し、（２）前記ｄ台の特定端末$T_{i1},\cdots,T_{id}$に対応した$Y_{i1},\cdots,Y_{id}$から、ｄ個の排除サブ情報
$C2_1=Y_{i1}^r$　（ＧＦ(p)上の演算），・・・，
$C2_d=Y_{id}^r$　（ＧＦ(p)上の演算）
を計算し、（３）前記ダミーの秘密鍵に対応した（ｋ－１）個の$Y_{n+1},\cdots,Y_{n+k-1}$から任意に（ｋ－ｄ－１）個の$Y_{i,d+1},\cdots,Y_{i,k-1}$の排除サブ情報
$C2_{d+1}=Y_{i,d+1}^r$　（ＧＦ(p)上の演算），・・・，
$C2_{k-1}=Y_{i,k-1}^r$　（ＧＦ(p)上の演算）
を計算し、特定端末のＩＤ番号$i_1,\cdots,i_d$と、ダミーのＩＤ番号$i_{d+1},\cdots,i_{k-1}$と、前記準備情報C1と、上記（ｋ－１）個の排除サブ情報$C2_1,\cdots,C2_{k-1}$を前記排除情報として求め，前記複数台の端末に同報通信し、前記センタは、
$K=Y^r$　（ＧＦ(p)上の演算）
を前記グループ鍵として求め、前記正規端末と前記不正端末以外のその他端末T_jが，前記排除情報から前記秘密鍵S_jを用いて前記グループ鍵を求める際は、
$\Lambda=\{j,i_1,\cdots,i_{k-1}\}$
とし、$\lambda(j,\Lambda),\lambda(i_1,\Lambda),\cdots,\lambda(i_{k-1},\Lambda)$を求め、前記準備情報C1と前記排除サブ情報$C2_1,\cdots,C2_{k-1}$と自身の前記秘密情報$S_j$を用いて、
$C1^{(S_j\times\lambda(j,\Lambda)\ \mathrm{mod}\ q)}\times C2_1^{(\lambda(i_1,\Lambda)\ \mathrm{mod}\ q)}$
$\times\cdots\times C2_{k-1}^{(\lambda(i_{k-1},\Lambda)\ \mathrm{mod}\ q)}$　（ＧＦ(p)上の演算）
を計算して、この結果をグループ鍵とすることを特徴とする請求項１記載の複製端末発見方法。
【請求項６】　前記センタは、正規端末T_iには、前記センタ暗号文EC_i^bの計算および送信はせずに、前記端末T_iを排除端末に含めた排除情報を、零でないＧＦ(q)の元ｒに代えて、前記端末T_i発生の乱数R_i^bに置き換えて生成して同報通信し、前記端末T_iでは，前記排除情報のうちの準備情報から、個別の秘密鍵S_iと前記乱数R_i^bを用いてグループ鍵を求めることを特徴とする請求項５記載の複製端末発見方法.
【請求項７】　前記ラウンド番号ｂにおけるグループ鍵GK^bを用いて、前記センタは、
$g'=g^{(1/GK^b)}$　（ＧＦ(p)上の演算）
を前記ｇに置き換え、前記正しい端末T_iは、
$S_i'=S_i\times GK^b$　（ＧＦ(q)上の演算）
を前記秘密鍵S_iに置き換えることにより、センタはラウンド番号ｂで排除した端末を、これ以降のラウンドにおいても排除しつづけることを特徴とする請求項５記載の複製端末発見方法。
【請求項８】　ｍ台の鍵生成機関A_jは，それぞれ秘密鍵SS_jを生成し、各端末T_iは、
$SS_j=\Sigma\lambda(i,\Lambda)\times SS_{i,j}$（和はｉ∈Λについて行なう）
（ただし、
$SS_{i,j}=SS_j+f_{1,j}\times i+\cdots+f_{k-1,j}\times i^{k-1}\ \mathrm{mod}\ q$
（$f_{1,j},\cdots,f_{k-1,j}$は、（ｋ－１）個のＧＦ(q)の元、ただし、$f_{k-1,j}\neq 0$）
$\lambda(i,\Lambda)=\Pi\{L/(L-i)\}$（積はL∈Λ－{ｉ}について行なう）
Λは、前記ｎ台の端末およびダミーから選んだ任意のｋ台からなる集合）を満たすｍ個の個別の秘密鍵$SS_{i,j}$を秘密に保持しており、これより
$S_i=\Sigma SS_{i,j}\ \mathrm{mod}\ q$（和は１≦ｊ≦ｍについて行なう）
で求めたS_iを前記端末秘密鍵S_iとして保持し、前記センタCは、
$YY_{i,j}=g^{SS_{i,j}}$　（ＧＦ(p)上の演算）
$Y_i=\Pi YY_{i,j}$　（ＧＦ(p)上の演算）（積は、１≦ｊ≦ｍについて行なう）
で求めたY_iを前記端末公開鍵Y_iとして保管することを特徴とする請求項５記載の複製端末発見方法。
【請求項９】　前記（Ｙ，Y_1，．．Y_{n+k-1}）を公開簿に登録して、前記センタに代わって、前記端末T_iが前記準備情報と前記排除サブ情報を生成して、これを同報通信することを特徴とする請求項５記載の複製端末発見方法。
【請求項１０】　前記排除情報の生成と排除情報からグループ鍵を求める際の乗法演算を、任意の有限体上の楕円曲線などの曲線上の加法演算に対応させることを特徴とする請求項５記載の複製端末発見方法。
【請求項１１】　センタＣと個別の識別子を保持するｎ台の端末（ｎは２以上の整数）からなり、センタが指定した端末を除いてグループ鍵を配送可能な同報通信システムにおいて、第１の秘密鍵をＳとし、前記第１の秘密鍵Ｓと前記台数ｎより大きい素数または素数のべき数をｐとし、（ｐ－１）の約数をｑとし、特定端末数をｄ（１≦ｄ＜ｎ－１）とし、前記各端末T_i（１≦ｉ≦ｎ）は、ｄ≦ｋ－２＜ｎを満たすｋを決定し、
$S=\Sigma\lambda(i,\Lambda)\times S_i$（和はｉ∈Λについて行なう）
（ただし、
$S_i=S+f_1\times i+\cdots+f_{k-1}\times i^{k-1}\ \mathrm{mod}\ q$
（$f_1,\cdots,f_{k-1}$は、（ｋ－１）個のＧＦ(q)の元、ただし、$f_{k-1}\neq 0$）
$\lambda(i,\Lambda)=\Pi\{L/(L-i)\}$（積はL∈Λ－{ｉ}について行う）
Λは、前記ｎ台の端末およびダミーから選んだ任意のｋ台からなる集合）を満たす個別の第１の秘密鍵S_iを秘密に保持しており、また、第２の秘密鍵をＵとし、
$V_i=g^{(U_i/S_i)}$　（ＧＦ(p)上の演算）
$U=\Sigma\lambda(i,\Lambda)\times U_i$（和はｉ∈Λについて行う）
（ただし、
$U_i=U+e_1\times i+\cdots+e_{k-1}\times i^{k-1}\ \mathrm{mod}\ q$

($e_1, \cdots, e_{k-1}$は$(k-1)$個のGF(q)の元、ただし、$e_{k-1} \neq 0$)
$\lambda(i, \Lambda) = \Pi\{L/(L-i)\}$ (積は$L \in \Lambda - \{i\}$について行なう)
Λは、前記n台の端末およびダミーから選んだ任意のk台からなる集合)を満たす個別の第2の秘密鍵V_iを秘密に保持しており、さらに(k-1)個の第1のダミーの秘密鍵を、
$S_{n+1} = S + f_1 \times (n+1) + \cdots + f_{k-1} \times (n+1)^{k-1} \bmod q$, ・・・,
$S_{n+k-1} = S + f_1 \times (n+k-1) + \cdots + f_{k-1} \times (n+k-1)^{k-1} \bmod q$
により計算して、同様に、
$U_{n+1} = U + e_1 \times (n+1) + \cdots + e_{k-1} \times (n+1)^{k-1} \bmod q$, ・・・,
$U_{n+k-1} = U + e_1 \times (n+k-1) + \cdots + e_{k-1} \times (n+k-1)^{k-1} \bmod q$
を計算して、前記センタCは、前記(S, p, q, g, S_1, ・・・, S_{n+k-1}, U_1, ・・・, U_{n+k-1})を保持し、前記端末T_iは、前記(S_i, V_i, p, q, g)を保持し、前記センタは、前記すでに前記グループ鍵GKを暗号化して送信した端末と、前記端末認証文の検証結果が正しくない、あるいは前記データベースに重複登録がある合計d台の特定端末$T_{i1}, \cdots, T_{id}$を排除するために、
(1)零でないGF(q)の元rを求めて、準備情報
$C1 = g^r$ (GF(p)上の演算)
を計算し、(2)前記d台の特定端末$T_{i1}, \cdots, T_{id}$に対応した第1の秘密鍵$S_{i1}, \cdots, S_{id}$と$U_{i1}, \cdots, U_{id}$から、d個の排除サブ情報
$C3_1 = r \times S_{i1} + U_{i1} \bmod q$, ・・・,
$C3_d = r \times S_{id} + U_{id} \bmod q$
を計算し、(3)前記ダミーの秘密鍵$S_{n+1}, \cdots, S_{n+k-1}$と$U_{n+1}, \cdots, U_{n+k-1}$から任意に(k-d-1)個ずつ選んで、これらを$S_{id+1}, \cdots, S_{ik-1}, U_{id+1}, \cdots, U_{ik-1}$として、以下の(k-d-1)個の排除サブ情報
$C3_{d+1} = r \times S_{i,d+1} + U_{i,d+1} \bmod q$・・・,
$C3_{k-1} = r \times S_{i,k-1} + U_{i,k-1} \bmod q$
を計算し、特定端末のID番号$i_1, \cdots, i_d$と、ダミーのID番号$i_{d+1}, \cdots, i_{k-1}$と、前記準備情報C1と、上記(k-1)個の排除サブ情報$C3_1, \cdots, C3_{k-1}$を前記排除情報として求め、前記複数台の端末に同報通信し、前記センタは、
$K = g^{\wedge}(r \times S + U)$ (GF(p)上の演算)
を前記グループ鍵として求め、前記正規端末と前記不正端末以外のその他端末T_jが、前記排除情報から前記秘密鍵S_jとV_jを用いて前記グループ鍵を求める際は、
$\Lambda = \{j, i_1, \cdots, i_{k-1}\}$とし、$\lambda(j, \Lambda), \lambda(i_1, \Lambda), \cdots, \lambda(i_{k-1}, \Lambda)$
を求め、前記準備情報C1と前記排除サブ情報$C3_1, \cdots, C3_{k-1}$と自身の前記秘密情報S_jとV_jを用いて、
$W1 = S_j \times \lambda(j, \Lambda)$
$W2 = C3_1 \times \lambda(i_1, \Lambda) + \cdots + C3_{k-1} \times \lambda(i_{k-1}, \Lambda) \bmod q$
$K = (C1 \times V_j)^{\wedge} W1 \times g^{\wedge} W2$ (GF(p)上の演算)
を計算して、この結果Kをグループ鍵とすることを特徴とする請求項1記載の複製端末発見方法。
【請求項12】 前記端末に前記排除情報を入力して、その結果のグループ鍵を観測することにより、端末内にある秘密鍵を推測することを特徴とする請求項1記載の複製端末発見方法。
【請求項13】 センタCと複数台の端末T_i(iは端末ID)を含むグループ同報通信システムの複製端末発見方式において、
前記端末T_iは、ラウンドbにおける端末乱数R_i^b(上付きbはラウンド番号を示す添字)を生成する端末乱数生成手段と、前記センタCから受信したセンタ乱数Z^bと前記端末乱数R_i^bに対する端末認証文D_i^bを端末秘密鍵S_iにより生成する認証文生成手段と、前記端末認証文D_i^bと前記端末乱数R_i^bをセンタ公開鍵Ycで暗号化して端末暗号文E_i^bを生成する公開鍵暗号化手段と、前記端末暗号文E_i^bを送信する端末側送信手段と、前記センタ暗号文EC_i^bを前記端末乱数R_i^bを用いて復号化してグループ鍵GKを得る第1のグループ鍵計算手段と、前記センタCから受信した排除情報と前記端末T_iの秘密鍵S_iを用いて、前記グループ鍵GKを得る第2のグループ鍵計算手段とを備え、
前記センタCは、グループ鍵K^bを生成するグループ鍵生成手段と、前記センタ乱数Z^bを生成するセンタ乱数生成手段と、前記センタ乱数Z^bをチャレンジCHAとして前記複数台の端末に送信するセンタ側送信手段と、センタ秘密鍵Scで前記端末暗号文E_i^bを復号して前記端末認証文D_i^bと前記端末乱数R_i^bを得る公開鍵暗号復号手段と、前記端末認証文D_i^bを端末公開鍵Y_i(センタが端末秘密鍵を管理している場合は端末秘密鍵S_i)で検証する認証文検証手段と、前記端末乱数R_i^bと前記端末T_iの端末IDとを対応させて登録するデータベース手段と、前記データベースを検索して同一端末IDでかつ異なる端末乱数が登録されている重複登録を検出する検出手段と、前記端末認証文D_i^bの検証結果が正しく、かつ前記重複登録が無い前記端末T_i(正規端末)の前記端末乱数R_i^bを用いて前記グループ鍵GKを暗号化した前記センタ暗号文EC_i^bを生成するグループ鍵暗号化手段と、前記すでに前記グループ鍵GKを暗号化して送信した端末と、前記端末認証文D_i^bの検証結果が正しくない、あるいは前記重複登録がある端末T_i(不正端末)と正規端末を排除してグループ鍵を共有するための排除情報を生成する排除情報生成手段と、前記センタ暗号文EC_i^bあるいは前記排除情報を前記複数台の端末に同報送信する送信手段とを備えたことを特徴とする複製端末発見方式。

【請求項１４】　前記排除情報生成手段は、現用グループ鍵を必要条件として新しいグループ鍵を生成するためのグループ鍵情報を生成する手段を備え、前記その他の端末は、現用のグループ鍵と配布されたグループ鍵情報を使って新しいグループ鍵を得る手段を備えたことを特徴とする請求項１３記載の複製端末発見方式。

【請求項１５】　前記認証文生成手段および前記認証文検証手段を、ディジタル署名を用いる手段としたことを特徴とする請求項１３記載の複製端末発見方式。

【請求項１６】　前記認証文生成手段および前記認証文検証手段を、鍵付きハッシュまたは共通鍵暗号を用いたメッセージ認証符号（ＭＡＣ）を用いる手段としたことを特徴とする請求項１３記載の複製端末発見方式。

【請求項１７】　前記公開鍵暗号化手段と前記公開鍵暗号復号手段に代えて、Diffie-Hellman鍵共有法を含む乱数を用いた鍵共有法の１つを用いて鍵を共有する手段と、共有した鍵を改めて端末乱数として用いる手段とを設けたことを特徴とする請求項１３記載の複製端末発見方式および排除方式。

【請求項１８】　前記センタＣに、前記センタ暗号文EC_i^bにメッセージ認証符号（ＭＡＣ）を含める手段を設け、前記端末T_iに、前記メッセージ認証符号を用いて改ざんや成りすましを検出する手段を設けたことを特徴とする請求項１３記載の複製端末発見方式。

【請求項１９】　前記センタＣに、前記センタ暗号文EC_i^bにディジタル署名を含める手段を設け、前記端末T_iに、前記ディジタル署名を用いて改ざんや成りすましを検出する手段を設けたことを特徴とする請求項１３記載の複製端末発見方式。

【請求項２０】　同一ラウンドにおいて前記グループ鍵が複数種類存在する場合に、前記端末T_iに前記端末暗号文E_i^bに所望のグループ鍵の種類を指定する手段と、同一ラウンドにおいては常に同じ前記端末乱数R_i^bを前記端末暗号文E_i^bに使用する手段とを設け、前記センタＣに、同一ラウンドにおいて同一の前記端末乱数R_i^bが使用された前記端末暗号文E_i^bにおいて指定された種類のグループ鍵を、前記端末乱数R_i^bを用いて暗号化して配送する手段を設け、また前記データベースをグループ鍵の種類ごとに管理したことを特徴とする請求項１３記載の複製端末発見方式。

【請求項２１】　前記端末T_iに、前記センタＣからの通信を受信できない場合に前記センタＣに対して現在のグループ鍵識別番号を問い合わせる問い合わせ手段と、前記端末T_iと前記センタＣの前記グループ鍵識別番号が異なる場合に前記センタＣに再送を要求する再送要求手段とを設けたことを特徴とする請求項１３記載の複製端末発見方式。

【請求項２２】　前記センタ公開鍵Ｙｃと前記センタ秘密鍵Ｓｃと前記端末公開鍵Y_iと前記端末秘密鍵S_iとを生成する手段と、前記センタ公開鍵Ｙｃを全端末に配布する手段と、前記センタ秘密鍵Ｓｃとすべての前記端末公開鍵Y_iとを前記センタＣに配布する手段と、前記端末秘密鍵S_iを対応する前記端末T_iに配布する手段とを有する信頼できるシステム管理手段を前記通信システムに備えたことを特徴とする請求項１３記載の複製端末発見方式。

【請求項２３】　前記端末乱数生成手段は、同じ乱数を出力する乱数生成器を他に作成できず、かつ偶然他の乱数生成器の出力と同じ出力となる確率が無視できる出力長を持つという条件を満たすことを特徴とする請求項１３記載の複製端末発見方式。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、複製端末発見方法に関し、特に、センタと複数の端末からなる通信システムにおける複製端末の存在を自動的に発見する複製端末発見方法に関する。

【０００２】

【従来の技術】センタと複数の端末からなる通信システムにおいて、情報の秘匿や端末の認証を行なう方法として、以下のような方法がある。すなわち、センタは、グループ鍵で端末に暗号化通信を行なう。端末は、予め格納された個別の秘密鍵を用いてグループ鍵を生成または入手して、センタからの暗号通信を復号する。センタは、端末の秘密鍵で作成された認証情報を検査して端末認証を行なう。

【０００３】このような方法では、秘密鍵をいかに安全に端末に格納するかが問題となる。そこで、不正なアクセスを物理的に困難にする対タンパー性を備えた耐タンパーデバイスに、秘密鍵を格納することが多く行なわれている。一般的に、耐タンパーデバイスとしてICカードが用いられる。ICカードに端末固有の秘密鍵を保持し、端末にこのICカードを挿入して使用する方式が、GSM方式の携帯電話や有料衛星放送のSTBなどに実装されている。

【０００４】しかしながら、近年はICカードに対する攻撃の研究が進み、ICカードの消費電流などから内部の秘密鍵を解読するPower Analysis Attacksなどが考案されており、ICカードの安全性は充分ではない。秘密鍵が漏洩した場合は、秘密鍵を用いた複製端末の偽造が可能になる。複製端末による暗号通信の傍受を防ぐために、暗号通信を中止して、複製端末を排除するなどの対策を講じなくてはならない。

【０００５】複製端末を発見する方法としては、暗号通信の内容が外部に漏れていることから推測する方法や、ブラックマーケットにおいて複製端末を定期的に調査するといった方法があった。このような方法は、発見の確実性が低く、発見までの時間もかかるうえ、人手によらず自動的に行なうことが困難である。

【０００６】これに対処するために、複製端末を事前に

検出する方法が、文献１［松下達之,渡邉祐治,古原和邦,今井秀樹,“ITSに適したコンテンツ配信における不正加入者の事前検出法,”2000年暗号と情報セキュリティシンポジウム,SCIS2000-C09,2000.］で提案されている。

【０００７】

【発明が解決しようとする課題】しかし、上記従来の事前検出法では、センタは基本的に端末を１台ずつチェックして、合格した端末にはグループ鍵を渡している。そのため、グループ内の端末が多い場合には、正しい端末全体に新しいグループ鍵を渡すまでの時間がかかる。特に、正しくない端末の存在が見つかったとき、新しいグループ鍵をこの端末を除いた全員で共有するまでの時間がかかり、センタは長い間暗号通信をとめなければならない。

【０００８】本発明は、上記従来の問題を解決して、複製端末を効率的に発見したあと、できるだけ早くその端末を排除してグループ鍵を共有することを目的とする。

【０００９】

【課題を解決するための手段】上記の課題を解決するために、本発明では、センタと複数台の端末を含むグループ同報通信システムの複製端末発見方法を、センタは、センタ乱数を生成し、グループ鍵の更新通知とセンタ乱数をチャレンジとして同報通信を用いて複数台の端末に送信し、チャレンジを受信した端末は、ラウンドごとに端末乱数を生成し、センタ乱数と端末乱数に対する端末認証文を端末秘密鍵により生成し、端末認証文と端末乱数とをセンタ公開鍵で暗号化して端末暗号文としてセンタに送信し、センタは、グループ鍵を生成し、センタ秘密鍵で端末暗号文を復号して端末認証文と端末乱数とを得て、端末公開鍵（センタが端末の秘密鍵を管理している場合は秘密鍵）で端末認証文を検証し、端末乱数と、端末の端末ＩＤとを、対応させて登録したデータベースを検索して、同一端末ＩＤでかつ異なる端末乱数が登録されている重複登録の有無を検査し、端末認証文の検証結果が正しく、かつ重複登録が無い前記端末（正規端末と称する）の端末乱数と端末ＩＤをデータベースに登録し、この正規端末の端末乱数を用いて、グループ鍵を暗号化してセンタ暗号文として正規端末に送信し、端末認証文の検証結果が正しくないか、重複登録がある端末（不正端末と称する）とすでに前記グループ鍵を暗号化して送信した正規端末とを排除してグループ鍵を共有するための排除情報を求めて、排除情報を同報通信で送信し、正規端末は、センタ暗号文を受信し、端末乱数を用いてこれを復号してグループ鍵を得て、正規端末と不正端末以外のその他端末の端末は、センタから排除情報を受信し、端末の秘密鍵を用いてグループ鍵を得て、不正端末は、センタ暗号文あるいは排除情報を用いても、グループ鍵を得ることができずにグループ同報通信から排除される構成とした。

【００１０】このように構成したことにより、端末はラウンドごとのグループ鍵を入手するために、センタ乱数と端末乱数に対する認証文を自身の秘密鍵により生成し、端末乱数と認証文をセンタの公開鍵により暗号化してセンタに送信しなければならないので、センタは同一ラウンドにおいて同じ端末秘密鍵をもつ端末から異なる端末乱数が送られてきた場合に複製端末の存在を発見できる。複製端末の存在を発見した場合、センタはこの端末を排除してグループ鍵を配送する。このとき、センタは正しい端末が生成した端末乱数を用いたセンタ暗号文、あるいは未チェックの端末に効率よく同じグループ鍵を配送するための排除情報を同報通信する。正しい端末では、センタ暗号文を自身の端末乱数を用いて復号してグループ鍵を求める。あるいは、未チェックの端末では、排除情報と秘密鍵を用いて（端末乱数は必要ない）所定の演算を行い前記グループ鍵を求める。排除情報は、排除する端末数に依存した容量の情報にすることが可能であり、未チェックの端末に対して効率よくグループ鍵を配布し、複製端末を除いた全員で早急にグループ鍵を共有できる。センタ側で複製端末の存在が確認された端末、認証の結果が不正であった端末、および発見を恐れて端末乱数を送らない端末には、センタは、センタ暗号文は送らず、また排除情報においても、これらの端末は排除するため、これらの端末は秘密情報を入手できない。

【００１１】また、認証文生成手段および認証文検証手段を、ディジタル署名方式とした。このような構成にしたことにより、センタは、各端末の秘密鍵を直接管理する必要がなく、管理が容易となり、かつセンタの不正による端末の陥れを防ぐことができる。

【００１２】また、認証文生成手段および認証文検証手段を、鍵付きハッシュまたは共通鍵暗号を用いたメッセージ認証符号（MAC）方式とした。このような構成にしたことにより、センタは認証文の検証を高速に行なうことができる。センタが信頼できるという前提があれば、端末とその乱数の認証にMACを利用できるので、通信量と演算量を最小限に抑えられる。

【００１３】また、公開鍵暗号化手段および公開鍵暗号復号手段の代わりに、乱数を用いた鍵共有法（例えばDiffie-Hellman鍵共有法）を用いて共有した鍵を乱数として用いる構成とした。このような構成にしたことにより、端末とセンタが平等に乱数を生成することができる。

【００１４】また、センタ暗号文にMACを含ませて改ざんや成りすましを検出する構成とした。このような構成にしたことにより、改ざんや成りすましを高速に検出できる。

【００１５】また、センタ暗号文にディジタル署名を含ませて改ざんや成りすましを検出する構成とした。このような構成にしたことにより、センタは各端末の秘密鍵

を管理することなく改ざんや成りすましを検出できる。

【００１６】また、１ラウンドにおいて秘密情報が複数種類存在する場合、端末が端末暗号文に所望の秘密情報の種類を指定し、かつ同一ラウンドにおいては常に同じ端末乱数を端末暗号文に使用し、センタは、同一ラウンドにおいて同一の端末乱数が使用された端末暗号文に対して指定された種類の秘密情報を端末乱数より生成した共通鍵により暗号化して配送する構成とした。このような構成にしたことにより、秘密情報が複数種類存在しても複製端末を発見することができる。

【００１７】また、端末がセンタからの通信を受信できない場合、センタに対して現在のラウンド番号を問い合わせる問い合わせ手段を端末に備え、問い合わせた結果、端末とセンタのラウンド番号が異なる場合に、端末がセンタに再送を要求する再送要求手段とを備えた構成とした。このような構成にしたことにより、端末がセンタからの情報を受信できない場合にも、複製端末の発見および秘密情報の配布を再開できる。

【００１８】また、端末乱数生成手段を、同じ乱数を出力する乱数生成器を他に作成できず、かつ偶然他の乱数生成器の出力と同じ出力となる確率が無視できる出力長を持つという条件を満たすものとした。このような構成にしたことにより、一定の攻撃に対して充分安全を確保できる。

【００１９】また、端末ｎ台を有する全体をｋ台ずつのサブグループごとにチェックし、サブグループのチェックの後に、未チェックの端末に対して排除情報を同報通信して、グループ鍵を更新する構成とした。このような構成にしたことにより、サブグループのチェックごとに新しいグループ鍵を、正しい端末および未チェックの端末で共有することができ、正しくない端末を排除して早急にグループ鍵を用いた暗号通信を行なうことができる。

【００２０】また、排除情報を生成する方法およびこれから端末秘密を用いてもとのグループ鍵を求める具体的な方法として、すでに知られている秘密分散法を利用した方法を用いる構成とした。この方法は、排除情報のデータ量が、全体の端末数には依存しないため（データ量は、排除する端末数に依存する）、この構成にしたことにより、特に大きなグループの際に効率的に排除情報を送信することができる。

【００２１】また、秘密分散法を利用した方法において、センタが生成する乱数の代わりに、端末からセンタに送信された乱数を用いる構成とした。この構成にしたことにより、センタからのセンタ暗号文の容量を削減することができる。

【００２２】また、すでに排除した端末を継続して排除するため、共有したグループ鍵を用いて排除端末以外では、端末秘密鍵を更新して、以降ではこれを用いて複製端末発見する構成とした。この構成にしたことにより、センタにおいて継続して排除する端末のデータベース管理を省くことができる。

【００２３】また、各端末の秘密鍵を複数の鍵生成機関で分散して行なう構成とした。この構成にしたことにより、センタ、あるいは各端末の秘密鍵の生成を一元管理する信頼のおける機関が存在しない場合であっても、システムを構成することができる。

【００２４】また、各端末の公開鍵を公開簿として実現し、どの端末もこの公開簿より確実にデータを取得できる構成にする。この構成にしたことにより、ラウンドごとに前記センタの役割を各端末で回り持ちすることができる。

【００２５】また、排除情報の生成方法を楕円曲線上の演算として構成にする。この構成にしたことにより、センタの計算量、センタからの排除情報のデータ量、端末での計算量を削減することができる。

【００２６】また、排除情報を生成する方法、およびこれから端末秘密を用いてもとのグループ鍵を求める別の具体的な方法として、すでに知られている２つの秘密情報と秘密分散法を利用した方法を用いる構成とした。この構成にしたことにより、未チェックの端末が排除情報からグループ鍵を求める際に、その計算量を大幅に削減することができる。

【００２７】また、端末に任意の排除情報を入力して所定のグループ鍵が出力されるかを確認する構成にする。この構成にしたことにより、複製端末が管理者により押収されたとき、この端末のＩＤを容易に知ることができる。

【００２８】

【発明の実施の形態】以下、本発明の実施の形態について、図１～図６を参照しながら詳細に説明する。

【００２９】（実施の形態）本発明の実施の形態は、センタと複数台の端末が、グループ鍵を用いた暗号通信が可能となる同報通信網により接続された通信システムにおいて、センタが各端末に新規グループ鍵を配布する際に、端末で発生した乱数が複製困難なことを利用して端末IDの重複を検査することで複製端末を発見する方法である。センタは、正規端末には、端末で発生した乱数を用いてグループ鍵を暗号化し、未チェックの端末には、正規端末と発見した複製端末を排除したグループ鍵共有方法でグループ鍵を送信する。

【００３０】図１は、本発明の実施の形態における複製端末発見方法のシステム模式図である。図１において、センタＣは、各端末にグループ鍵を配布する組織である。センタＣと7台の端末は、同報通信可能な無線または有線の通信媒体で接続されている。端末T_iは、センタＣとグループ鍵で暗号通信を行なう通信装置である。端末は複数台あり、ｉは各端末にユニークな端末IDである。ここでは、検査対象の端末T_1～T_4のうち、端末T_1は正規端末、端末T_2は複製端末が存在し、端末T_3は

センタCに通信せず、端末T_4は端末秘密鍵を保持しない偽の端末とする。

【００３１】図２は、本発明の実施の形態における複製端末発見方法に用いるセンタの構成図である。図２において、乱数生成手段１は、擬似乱数を生成する手段である。送信手段２は、有線または無線でデータを端末に送信する手段である。公開鍵暗号復号手段３は、端末から送られた端末認証文を受け取り、センタCの公開鍵でこれを復号して、暗号化された認証文と端末が生成した乱数を獲得する手段である。認証文検証手段４は、端末秘密鍵で暗号化された認証文を端末公開鍵で復号して検証する手段である。データベース手段５は、端末との交信記録をまとめたデータベースである。検出手段６は、データベースを検索して端末の重複を検出する手段である。共通鍵暗号化手段８は、グループ鍵を端末の乱数を用いてグループ鍵暗号化する手段である。排除情報生成手段７は、複製端末および不正端末を排除して、排除情報を生成する手段である。

【００３２】図３は、本発明の実施の形態における複製端末発見方法に用いる端末の構成図である。図３において、乱数生成手段11は、端末において複製困難な擬似乱数を生成する手段である。送信手段12は、端末認証文を有線または無線を介してセンタに送信する手段である。第１のグループ鍵計算手段13は、センタから通信されたセンタ暗号文と、端末乱数を用いてグループ鍵を求める手段である。認証文生成手段14は、センタ乱数に対応して端末の乱数を用いて認証文を生成する手段である。公開鍵暗号手段15は、この認証文をセンタの公開鍵を用いて暗号化する手段である。第２のグループ鍵計算手段16は、センタから通信された排除情報と、秘密鍵17を用いてグループ鍵を求める手段である。

【００３３】図４は、本発明の実施の形態における複製端末発見方法の複製端末発見フェーズ（フェーズ＃１）の流れ図である。図５は、本発明の実施の形態における、センタと正規端末の複製端末発見方法のグループ鍵配送フェーズ（フェーズ＃２－Ａ）の流れ図である。図６は、本発明の実施の形態における、センタと未チェックのグループ鍵配送フェーズ（フェーズ＃２－Ｂ）の流れ図である。

【００３４】上記のように構成された本発明の実施の形態における複製端末発見方法の動作を説明する。最初に、図１を参照して、複製端末発見方法の原理を説明する。この複製端末発見方法では、センタCにしか解読できないように暗号化されて端末T_iから送信された端末乱数R_i^bと端末認証文を、センタCで検証し、端末認証文が正しく、かつ現時点において同じ端末IDを持つ端末から異なる端末乱数R_i^bが送信されていない場合にのみ、この端末乱数R_i^bに依存して端末T_iにグループ鍵GKを与える。ただし、上付きのｂはラウンド番号であり、ベキ乗の意味ではない。ラウンドは、全端末を検査する期間である。端末IDのｉやラウンド番号ｂを省略することもある。

【００３５】この複製端末発見方法は、複製端末発見フェーズ（フェーズ＃１）とグループ鍵配送フェーズ（フェーズ＃２）の２つのフェーズからなる。フェーズ＃１では、端末から乱数を生成してセンタに通知する。そしてデータベースを用いて重複登録をチェックする。センタは、端末T_2については、チェック検査履歴BHより同じ端末IDが存在して乱数が異なることにより複製端末の存在を発見する。また、端末T_4については、センタでの認証検証が失敗する。

【００３６】フェーズ＃２では、センタは、正しい端末と未チェックの端末に、生成したグループ鍵GKを送信する。正しい端末T_1には、端末T_1が生成した乱数で暗号化して端末T_1に送信する。同時に、検査対象以外、つまり未チェックの端末に対しては、対象の端末T_1～T_4を排除した排除情報を生成して同報通信する。端末T_1は、端末乱数を用いて暗号化グループ鍵を復号し、グループ鍵を求める。検査対象外の端末T_5～T_7は、排除情報と自身の秘密鍵を用いてグループ鍵を求める。一方、端末T_2～T_4は、グループ鍵を獲得できない。

【００３７】複製端末発見フェーズ（フェーズ＃１）では、センタCは、チャレンジ-レスポンス認証により、端末T_iと、その端末T_iがセンタCの公開鍵により暗号化して配信した端末乱数R_i^bを認証する。センタCは、データベースを検索して、端末識別符号（端末ID）の重複を検査する。同一端末IDを持ち、異なる端末乱数を送信した端末T_i'を検出すると、この端末IDを持つオリジナル端末T_iの複製端末が存在すると判定できる。グループ鍵配送フェーズ（フェーズ＃２－Ａ）では、センタCは、複製端末のない端末T_iに対して、グループ鍵GKを端末乱数により暗号化して配送する。対応する端末では、自身が発生した端末乱数を用いて、第１のグループ鍵計算手段によりグループ鍵を求める。複製端末の存在が発見されたときには、センタCは未チェックの端末に対して、複製端末を排除した排除情報を同報通信網で配送する。これを受信した未チェックの端末は自身の秘密鍵を用いて、第２のグループ鍵計算手段によりグループ鍵を求める。

【００３８】チャレンジ-レスポンス認証を説明する。センタCは、センタ乱数Z^bを生成して、チャレンジCHAとして端末T_iに送信する。端末T_iは、センタCから受信したセンタ乱数Z^bと、自身が生成した端末乱数R_i^bに対して、自身の秘密鍵により生成した認証文を、レスポンスRESとしてセンタCに送信する。これをセンタCが検証することにより、端末T_iとその端末乱数R_i^bを認証する。ここで、センタCは、端末T_iとその端末乱数R_i^bとの対応を確認する。ディジタル署名を用いる場合は、センタCに各端末の秘密鍵を保管する必要がなく、鍵管理が容易となる。なお、ここでセンタCは、チ

ャレンジデータに対するレスポンスデータで端末の認証を行っているが、リプレイ攻撃の危険がない場合には、センタCからのチャレンジを省略して、端末が独自で生成した端末乱数に対するディジタル署名を端末からセンタCに送ることにより、センタCで認証を行なう。

【００３９】端末乱数R_i^bの暗号化を説明する。同じ端末秘密鍵を保持する複製端末に対して端末乱数R_i^bを秘密にするために、センタ公開鍵により端末乱数R_i^bを暗号化する。または、Diffie-Hellman鍵共有法のような乱数を用いた方法により共有した鍵を、端末乱数の代わりに利用する。

【００４０】データベースの検索を説明する。センタCは、データベースを検索して、端末T_iに既にグループ鍵GKを配送済みか確認する。配送済みならば、配送に使用した端末乱数R_i^b'と、送信されてきた端末乱数R_i^bとを比較して、不一致ならば、端末T_iの複製端末が存在すると判断する。端末T_iは、同一ラウンドでは同じ乱数を用いるので、複製端末が存在しない限り、異なる端末乱数R_i^bを用いたレスポンスRES_i^bは来ない。ただし、端末乱数R_i^b'と端末乱数R_i^bのどちらが複製端末の乱数であるかは区別できない。また、複製端末が複数ならば、端末乱数R_i^b'と端末乱数R_i^bが共に複製端末の乱数である可能性があるが、複製端末が単数複数いずれの場合でも、複製端末発見方法により複製端末の存在を検出できる。

【００４１】グループ鍵GKの暗号化を説明する。センタCは、端末が生成した端末乱数を用いて、グループ鍵を暗号化する。端末T_iは、端末乱数を使ってグループ鍵を復号する。端末秘密鍵S_iが漏洩しても、端末乱数R_i^bがなければ、オリジナル端末と複製端末の集合の中で、グループ鍵を得ることができるのは、１台のみとなる。また、ここで使う暗号は、レスポンスRES_i^bの場合と異なり、共通鍵暗号でよい。また、必要であればMAC（Message Authentication Code：メッセージ認証符号）を併用して、改ざんや成りすましを検出する機能を追加できる。

【００４２】グループ鍵の更新を説明する。センタCは、一時横流しによるグループ鍵の漏洩に対処するために、定期的にグループ鍵を更新して、複製端末発見方法を実行する必要がある。この期間が短いほど、早く複製端末を発見・無効化できる。全端末を複数のサブグループに分けて、サブグループごとに複製端末のチェックを行なう場合は、サブグループのチェックごとにグループ鍵を更新する。さらに、正規端末の複製端末が存在して送信を行なわない場合は、その複製端末を排除するために、前回のグループ鍵を使って新しいグループ鍵を得るようにする。すなわち、排除情報で同報送信するグループ鍵情報を、前回のグループ鍵で復号するか、前回のグループ鍵と配布したグループ鍵情報を合成して、新しいグループ鍵を得るなどの方法を使う。

【００４３】グループ鍵が複数の場合を説明する。グループ鍵の種類が複数の場合は、各端末T_iは、同一ラウンドであれば同じ端末乱数を用いて、グループ鍵の種類を指定したレスポンスRES_i^bを送信する。センタCは、データベースより端末乱数が同じことを確認して、端末T_iが指定したグループ鍵を、同じ端末乱数による鍵で暗号化して配送する。

【００４４】未受信対策を説明する。端末T_iが電源オフや、通信できない地域へ移動したことなどにより、チャレンジCHA^bやグループ鍵を受信できない場合のために、現在のグループ鍵識別番号をセンタに問い合わせる機能を、端末T_iに付加する。グループ鍵が更新されている場合に、端末T_iはセンタに再送を要求する。

【００４５】以上のようにすることにより、複製端末を発見できる。正規の端末T_iが先にレスポンスRES_i^bを送信し、複製端末がレスポンスRES_i^bを送信しない場合には、複製端末は発見できないが、複製端末はグループ鍵を得ることができないので、実質的に無効化することができる。

【００４６】第２に、図２、図３、図４を参照しながら、複製端末発見の手順（フェーズ＃１）の各ステップについて説明する。準備段階において、図示していない信頼できるシステム管理者は、センタ秘密鍵Scと、センタ公開鍵Ycと、各端末T_iの端末秘密鍵S_iと、端末公開鍵Y_iを生成する。センタCに、センタ秘密鍵Scと端末公開鍵Y_iを秘密に配布する。各端末T_iに、対応する端末秘密鍵S_iとセンタ公開鍵Ycを秘密に配布する。

【００４７】図４に示すフェーズ＃１－１で、図１に示すセンタCは、図２の乱数生成手段１でセンタ乱数Z^bを生成する。端末T_iに、チャレンジ

$CHA^b = Z^b$

を、送信手段２により送信する。

【００４８】フェーズ＃１－２で、図３に示す端末T_iは、図３の乱数生成手段１により、端末乱数R_i^bを生成する。自身の端末秘密鍵S_iを用いて、端末IDのｉと、センタCからチャレンジCHA^bとして送られたセンタ乱数Z^bと、端末乱数R_i^bとに対するディジタル署名SIG$(S_i, (i \| Z^b \| R_i^b))$を、認証文生成手段10で生成する。ただし、$(x \| y)$は、ｘを上位桁とし、ｙを下位桁とする、符号の連接を示す。SIG(ｘ,ｙ)は、鍵ｘを使ってｙのディジタル署名を計算することを示す。このディジタル署名を、端末認証文D_i^bとする。

【００４９】センタ公開鍵Ycを用いて、端末IDのｉと、端末乱数R_i^bと、端末認証文D_i^bとに対する端末暗号文

$E_i^b = Yc[i \| R_i^b \| D_i^b]$

$= Yc[i \| R_i^b \| SIG(S_i, (i \| Z^b \| R_i^b))]$

を、公開鍵暗号化手段15で生成する。ただし、ｘ[ｙ]は、ｙを鍵ｘで暗号化することを示す。これを、センタCに、グループ鍵要求通知を兼ねるレスポンス

$RES_i^b = E_i^b = Yc[i \| R_i^b \| D_i^b]$
$= Yc[i \| R_i^b \| SIG(S_i, (i \| Z^b \| R_i^b))]$
として、送信手段２で送信する。

【００５０】フェーズ＃１－３で、図２のセンタＣは、図示しない受信手段で、端末T_iからのレスポンスRES_i^bを受信し、公開鍵暗号復号手段３で、センタ秘密鍵Scを使ってレスポンスRES_i^bを復号して、端末乱数R_i^bを得る。認証文検証手段４で、端末T_iの端末公開鍵Y_iを用いて、$SIG(S_i, (i \| Z^b \| R_i^b))$を検証する。検証結果が正しい場合は、端末$T_i$と端末乱数$R_i^b$を認証したとして受付けて、フェーズ＃１－４へ進む。検証結果が不正の場合は、不正端末を発見したことになるので、不正端末を記録し、この端末のチェックは終了する。

【００５１】フェーズ＃１－４で、センタＣは、検出手段６により、端末IDをキーとして、端末IDとグループ鍵配送に用いた乱数を関連付けて登録したデータベースが格納されたデータベース手段５を参照する。配送に用いた乱数が登録されていない、つまりグループ鍵GKが未配送の場合は、データベースに端末乱数R_i^bグループ鍵を記録して、フェーズ＃１-５へ進む。配送に用いた乱数が登録されている、つまりグループ鍵GKが配送済みの場合は、データベースに記録された端末乱数R_i^b'と受信した端末乱数R_i^bが等しいならフェーズ＃１-５へ進む。異なるなら、複製端末を発見したと判断して、フェーズ＃２－Ｂに進む.

【００５２】フェーズ＃１－５で、センタＣは、端末乱数R_i^bを共通鍵CK_i^bとする。

【００５３】第３に、図２、図３、図５、図６を参照しながら、グループ鍵配送の手順（フェーズ＃２）の各ステップを説明する。フェーズ＃２－Ａでは、重複が検出されなかった端末に対してのみ、センタＣはグループ鍵を配送する。フェーズ＃２－Ｂでは、重複が検出された端末が存在したときに、その端末を排除した排除情報を配送する。これにより未チェックの端末がグループ鍵を求めることができ、グループ全体での不正端末を排除した暗号通信を早急に再開することができる。

【００５４】図５に示すフェーズ＃２－１で、センタＣは、グループ鍵GKを共通鍵CK_i^bで暗号化したセンタ暗号文
$EC_i^b = CK_i^b[GK^b]$
を生成して、送信手段２により端末T_iに送信する。

【００５５】フェーズ＃２－２で、端末T_iは、図示してない受信手段により、センタ暗号文EC_i^b（$=CK_i^b[GK]$）を受信する。端末乱数R_i^bを共通鍵CK_i^bとして、図３の第1のグループ鍵計算手段により、センタ暗号文EC_i^b（$=CK_i^b[GK]$）を復号し、グループ鍵GKを得る。端末T_iが、センタ暗号文EC_i^b（$=CK_i^b[GK]$）を受信できなかった場合は、フェーズ＃１-２において生成したレスポンスRES_i^bを、センタＣに再送する。

【００５６】図６に示すフェーズ＃３－１で、センタＣは複製端末が確認できた端末、認証が失敗した端末、乱数の配送がない端末を排除した排除情報を、未チェックの端末に同報通信する。フェーズ＃３－２aで、未チェックの端末は、排除情報と自身の秘密鍵を用いて図３の第２のグループ鍵計算手段により、グループ鍵を得る。

【００５７】第４に、乱数生成器の条件を説明する。端末に組込まれる乱数生成手段が満たすべき条件は、「同じ乱数を出力する乱数生成器を他に作成できないこと、かつ偶然他の乱数生成器の出力と同じ出力となる確率が無視できる出力長を持つこと」である。これは、乱数生成器の構造は複製できても、乱数またはシードの元となる状態が複製できないものであって、かつ出力が128bit程度あるものであれば満たされる。したがって、次の128bit乱数生成器は条件を満たす。

・ホワイトノイズなどを利用した真性乱数生成器
・予測困難な常に変化する各端末固有の状態により更新されるシードを入力とする擬似乱数生成器または擬似乱数生成ソフトウェア

【００５８】このようなシードとして、以下のものや、その組合せがある。

・端末のメモリの状態やシステムクロックの値
・端末の動作に関する時間，時刻，回数

【００５９】第５に、安全性について説明する。複製端末発見方法は、複製端末の発見を目的とする。攻撃者は複製端末を偽造して暗号通信を解読することを目的とする。まず、複製端末発見方法において想定される攻撃について説明する。複製端末発見方法では、既に攻撃者が複製対象となるオリジナル端末の秘密鍵を保持していることを前提とした攻撃を想定する。端末秘密鍵を不正に取得できる機会には、メンバが自身の端末を解析する場合と、メンバが自身の端末から目を離している間（紛失・充電時など）に攻撃者が端末を解析する場合と、複数のメンバの結託により他のメンバの秘密鍵を作成する場合などがある。この前提において、攻撃者は、複製端末を偽造して暗号通信の解読を試みる。

【００６０】攻撃は、オリジナル端末はそのままに、攻撃者が残りの秘密情報（グループ鍵、乱数）を入手できる横流し攻撃と、オリジナル端末を改変するか、別の端末（複製端末）に入れ替えてしまうことにより、オリジナル端末を無効化する改変攻撃に分けられる。

【００６１】横流し攻撃のうち、一時横流し攻撃では、ある時点において、オリジナル端末のグループ鍵か、このグループ鍵を得るための乱数が漏洩し、攻撃者が複製端末を偽造する。常時横流し攻撃では、定期的に、オリジナル端末のグループ鍵か、このグループ鍵を得るための乱数を、不正なメンバが横流しして、攻撃者が複製端末を偽造する。改変攻撃は、オリジナル端末を改変するか、複製端末に入れ替えることにより、オリジナル端末を無効化し、複製端末を使用しても発見させない攻撃である。

【００６２】本実施の形態における複製端末発見方法は、一時横流し攻撃に対して複製端末を発見することを目的とする。常時横流し攻撃および改変攻撃は、以下の理由により考慮する必要がないと考える。

【００６３】常時横流し攻撃は、横流しの頻度に依存して不正なメンバの通信コストや不正発覚の可能性が増加するため、不正なメンバは容易に実行できないと考えられる。

【００６４】改変として、具体的に以下の２つの場合が考えられる。１つ目は、オリジナル端末の使用者が目を離した隙などに、攻撃者がオリジナル端末を複製端末と入れ替える場合である。この複製端末は、他の複製端末と乱数が同期しているとすれば、改変されたオリジナル端末を使用し続ける限り、乱数による複製端末の発見はできない。しかし、常時端末を使用しているオリジナル端末の使用者に気付かれない複製端末を偽造することは、時間やコストの面から難しいと考える。また、物理的な改変を検出することは、情報の複製を検知することに比べ、一般に容易かつ低コストであるので、これを併用して対処できる。

【００６５】２つ目は、オリジナル端末の使用者が、攻撃者または攻撃者に協力する不正なメンバの場合である。オリジナル端末の乱数生成器を複製端末と同期するように改変するか、同期する複製端末に入れ替えることにより、オリジナル端末を無効化する。１つ目より、不正なメンバの協力により成功する可能性が高い。しかし、不正発覚時に所有する改変した端末または複製端末により、不正なメンバであることを特定されてしまうため、容易に実行できない。また、端末を故障させて常に同じ乱数を出力させることにより、複製端末と乱数生成器を同期させる攻撃は、一定期間ログを保存・解析することにより検出できる。

【００６６】以上の検討より、複製端末発見方法では、以下の仮定が満たされるとする。このとき、複製端末発見方法は安全である。

１．攻撃者は複製対象となる端末の秘密鍵を保持する。
２．一時横流し攻撃が可能である。
３．常時横流し攻撃および改変攻撃は困難である。
４．端末に上に定義した乱数生成器が組込まれる。
５．オリジナル端末はメンバにより使用される。
６．共通鍵暗号方式、公開鍵暗号方式、MACおよびディジタル署名方式は安全である。

【００６７】仮定１と２は現実的に起こりうる。一方、仮定３の攻撃は理論的には可能だが、攻撃者の負担が大きく、現実的にはあまり起こりえないと予測されるため考慮しない。仮定３～５により、オリジナル端末に対する入替えや改変は行われず、かつ前述の乱数生成器をメンバが必ず使用すると仮定できる。仮定６については、共通鍵暗号方式として鍵長128bit程度の共通鍵暗号を利用し、公開鍵暗号方式として鍵長1024bit程度のRSA暗号やElGamal暗号や、鍵長160bit程度の楕円ElGamal暗号を利用し、MACとして鍵長128bit程度の共通鍵暗号や、出力128bit程度の鍵付きハッシュ関数を利用し、ディジタル署名として鍵長1024bit程度のDSA署名やRSA署名や、鍵長160bit程度の楕円DSA署名を利用することにより満たされる。

【００６８】一時横流し攻撃に対する安全性について説明する。攻撃者が入手可能な情報は、オリジナル端末の秘密鍵と、攻撃に成功した時点のラウンドのグループ鍵と、対応する乱数である。以上により偽造された単数または複数の複製端末と、オリジナル端末が存在すると考える。

【００６９】攻撃時点のラウンドのグループ鍵が更新されたとき、オリジナル端末が先にレスポンスRESを送信し、後から複製端末がレスポンスRESを送信した場合は、乱数の違いから複製端末を発見できる。レスポンスRESを送信しなければ、複製端末はグループ鍵を得られないため、実質的に無効化される。一方、複製端末が先にレスポンスRESを送信し、後からオリジナル端末がレスポンスRESを送信した場合は、乱数の違いから複製端末を発見できる。

【００７０】つまり、オリジナル端末と複製端末の集合の内、グループ鍵を得られるのは常に１台であり、この内１台でもレスポンスRESを送信すれば、複製端末を発見または無効化できる。ここで、前述の仮定により、集合の内最低１台はレスポンスRESを送信するので、この攻撃に対して複製端末発見方法は安全である。

【００７１】他の攻撃に対する安全性について説明する。偽造以外には、レスポンスRESを再送するReplay Attackがある。レスポンスRESに対して、センタは、共通鍵により暗号化したグループ鍵を配送するので、通信量は増加するが、乱数が無ければ復号はできないので問題ない。また、仮定により、暗号化関数と認証文生成関数が安全なので、暗号文の解読・レスポンスRESに対する成りすまし・改ざんは困難である。改変攻撃で述べたような端末を故障させる攻撃に対しては、センタが過去のデータベースを記録・検査すれば対処できる。したがって、過去の全てのラウンドのデータベースを保持・検査することが最も安全であるが、実際にはコストと安全性のトレードオフで、一定期間のデータベースのみを保持することになる。センタによる端末の陥れに関しては、センタが端末の秘密鍵を保持していないために困難である。

【００７２】第６に排除情報の生成とこれを用いたグループ鍵の計算方法について説明する。排除情報の生成の方法としては、例えば、次の文献２に開示された方法を用いればよい。

文献２[J. Anzai, N. Matsuzaki, and T. Matsumoto, "A Quick Group Key Distribution Scheme with Entity Revocation," Advanced in Cryptology - ASIACRYPT'9

9, LNCS1716, pp. 333-347, Springer-Verlag, 1999.]この方法は、排除情報のデータ量がグループの端末数には依存せず、排除する端末に依存する。そのため、大きなグループで、複製端末を発見して排除するのに適している。

【００７３】この排除方法を用いた１つの実現方法を以下に示す。ここでは、グループ全体を小さなサブグループに分けて、サブグループごとに複製端末の存在をチェックしていく。最初に、セットアップ段階を説明する。システム管理者は、以下の手順でシステムパラメータと、センタと各端末の秘密鍵および公開鍵を生成する。

【００７４】１．システム管理者Aは、しきい値ｋ（０≦ｄ≦ｋ－２＜ｎ）を決定する。ここで、ｄは、チェック検査可能な端末数の上限値であり、ｎ台の端末をｄ台ずつ分けてチェック検査するものとする。

【００７５】２．システム管理者Aは、次の値を生成し、センタCと全端末T_iに配送する。ｐ（大きな素数）と、ｑ（ｐ－１を割り切る大きな素数（ｎ＋ｋ－１＜ｑ））と、ｇ（Zpにおける位数ｑの元）を生成して配送する。

【００７６】３．システム管理者Aは、システム秘密鍵Ｓ（∈Zq）を決定し、しきい値ｋの秘密分散法を用いて、以下のとおり（ｎ＋ｋ－１）個のシェアを生成する。

a.

$a_0=S$

b. Zqにおいて次式を定義する。a_1, a_2, …, a_{k-1}(0≦a_t≦q－1, 1≦t≦k－1, $a_{k-1}\neq 0$)は乱数とする。

$f(x)=a_f\times x^f \bmod q$

c. f(x)を用いて（ｎ＋ｋ－１）個のシェアを計算する。

$S_i=f(i)$（1≦i≦n＋k－1）

【００７７】４．システム管理者Aは、S_1, S_2, …, S_nを、それぞれT_1, T_2, …, T_nの秘密鍵として秘密に配送する。

【００７８】５．システム管理者Aは、次式により公開鍵を計算し、Y_1, Y_2, …, Y_nをT_1, T_2, …, T_nの公開鍵として、Y_{n+1}, Y_{n+2}, …, Y_{n+k-1}をダミーの公開鍵として、センタCに配送する。また、システム公開鍵Yを、センタCと全端末T_iに配送する。

$Y_i=g^{\wedge}(S_i) \bmod p$ （1≦i≦n＋k－1）

$Y=g^S \bmod p$

【００７９】６．システム管理者Aは、センタの秘密鍵S_cと公開鍵Y_cを生成し、秘密鍵S_cをセンタCに秘密に配送し、公開鍵Y_cを全端末T_i に配送する。

【００８０】次に、ラウンドｂにおけるｗ番目のチェック対象サブグループの検査方法を説明する。フェーズ＃１（複製端末発見フェーズ）では、サブグループ内の各ｄ台の端末それぞれと、端末乱数を用いたセッションを確立し、もし存在していれば複製端末を発見する。

【００８１】〔フェーズ＃１－１〕センタCは、検査履歴BHを参照して、ラウンドｂにおいて、まだ検査していないｄ（≦ｋ－２）台の端末T_iを決定し、これらをｗ番目の検査対象端末とする。以下の手順では、検査対象端末のIDの集合Λを、正規端末のID集合Λ_1と不正端末のID集合Λ_2に選り分ける。

$\Lambda=\Lambda_1\cup\Lambda_2$, $\Lambda_1\cap\Lambda_2=\phi$（空集合）

が成り立つものとする。

【００８２】〔フェーズ＃１－２〕センタCは、ラウンドごとにチャレンジCHAを生成し、集合ΛにIDを持つ全端末T_iへ、更新通知

$CHA=(\Lambda \| Z^b)$

を同報で送信する。

【００８３】〔フェーズ＃１－３〕各端末T_i（i∈Λ）は、乱数R_i^bを生成し、以下のレスポンスRES_iをセンタCに送信する。RES_iには、フェーズ＃１－２の更新通知に対する端末T_iの認証文と、乱数R_i^bをセンタの公開鍵で暗号化した暗号文が含まれる。

$RES_i=Yc(i \| R_i^b \| SIG(i \| Z^b \| R_i^b))$

【００８４】〔フェーズ＃１－４〕センタCは、秘密鍵S_cを用いてRES_iを復号し、乱数R_i^bを求める。そして、更新通知に対するレスポンスの正当性を確認する。レスポンスが不正である場合、センタは端末のIDを集合Λ_2に移動して、フェーズ２の処理に移行する。一方、正当である場合には、乱数R_i^bを端末T_iとのセッション鍵とする。

【００８５】〔フェーズ＃１－５〕センタCは、Λ内の各端末の検査履歴BHを参照して、以下のとおり、正しい端末のIDは集合Λ_1へ、不正な端末のIDは集合Λ_2に移動する。ラウンドｂにおいて未検査の場合は、検査履歴BHに検査済みフラグと乱数R_i^bを記録し、ｉを集合Λ_1に移動する。ラウンドｂにおいて検査済みの場合は、記録されている乱数とR_i^bが異なるなら、複製端末を発見したと判断してｉを集合Λ_2に移動する。同じ場合は、ｉを集合Λ_1に移動する。

【００８６】〔フェーズ＃１－６〕センタCは、乱数Rhを生成して、次式よりグループ鍵GK_w^bを計算する。

$GK_w^b=Y^{\wedge}(Rh)$　(GF(p)上の演算)

【００８７】フェーズ＃２（グループ鍵配送フェーズ）では、不正端末を排除した排除情報を、未チェックの端末に配送して、サブグループ以外のグループ鍵を更新すると共に、サブグループ内の正規の端末には、確立したセッション鍵を用いてグループ鍵を個別配送する。

【００８８】〔フェーズ＃２－１〕センタCは、集合｛ｎ＋１, ｎ＋２, …, ｎ＋ｋ－１｝から任意に（ｋ－ｄ－１）個の整数を選び、その集合をΘとする。

【００８９】〔フェーズ＃２－２〕センタCは、乱数ｈと公開鍵Y_i（i∈Λ∪Θ）を用いて、次式より準備情報Ｘと（ｋ－１）個の排除情報M_iを計算する。

$X=g^{\wedge}(Rh)$　(GF(p)上の演算)
$M_i=Y_i^{\wedge}(Rh)$　(GF(p)上の演算)　($i\in\Lambda\cup\Theta$)
【００９０】[フェーズ＃２－３]センタＣは、集合Λ_1内の端末とのセッション鍵で、グループ鍵を暗号化する。
$EGK_w^b=Enc(R_i^b,(GK_w^b))$　(5)
【００９１】[フェーズ＃２－４]センタＣは、排除情報および暗号化グループ鍵情報を、センタの署名を付加して送信する。
【００９２】[フェーズ＃２－５]各端末T_iは、センタの公開鍵Y_cを用いて、排除情報を検証する。成功ならば、各端末T_i($i\in\Lambda_1$)は、乱数R_i^bを用いて、グループ鍵を獲得する。
$GK_w^b=Dec(R_i^b,EGK_w^b)$
[フェーズ＃２－６]未チェックの各端末T_i(iは、($\Lambda\cup\Theta$)に属さない)は、秘密鍵S_iを用いて、次式よりグループ鍵GK_w^bを計算する。
$GK_w^b=X^{\wedge}(S_i\times L(\Lambda\cup\Theta\cup\{i\},i)\times\Pi M_j^{\wedge}L(\Lambda\cup\Theta\cup\{i\},j)$(積は、$j\in(\Lambda\cup\Theta)$)$=X^{\wedge}S$ (GF(p)上の演算)
なお、ここで、Ｌ関数は、ラグランジェの補間係数であり、Ψを任意の集合、ｕを任意の整数としたとき、次のように表される。
$L(\Psi,u)=\Sigma\{t/(t-u)\}\ mod\ q$ (和は、$t\in(\Psi-\{u\})$)
【００９３】サブグループの検査が終了して、今回検査したサブグループの端末を排除して、未検査の端末と、前回までに検査したサブグループの端末に、新しいグループ鍵を同報通信する場合には、配布した情報から前回のグループ鍵を使って新しいグループ鍵を得るように、センタでグループ鍵情報を生成して配布する。こうすることにより、正規端末と同じ端末秘密鍵を持ち、レスポンスを返さない不正端末も、継続的に排除することができる。
【００９４】上記の方法を、次のように拡張することができる。
１．センタ通信量の削減
乱数Rhを、センタ作成のものに代えて、チェック検査対象の端末T_i発生の乱数R_i^bに置き換える。このとき、排除情報のうち、端末T_i分のEGK_w^bは送らなくてもよい。端末T_iは、乱数R_i^bを用いて、グループ鍵$Y^{\wedge}R_i^b\ (mod\ p)$を求める。
【００９５】２.複製端末の継続排除
以前のグループ鍵Ｋを用いて、正しい端末T_iにおいては、秘密鍵を、$S_i\times K\ mod\ q$に置き換え、一方センタにおいて、ｇを、$g^{1/K}\ mod\ p$に置き換えることにより、このラウンドで排除した端末を集合Λ2に含めることなく、永久に排除することもできる。
【００９６】３.排除のタイミング
サブグループ単位で検査と端末排除を行っているが、これを例えば、1台ずつ検査を行い、排除すべき端末が見つかった時点で、すぐに端末排除方法を用いてグループ鍵を更新すると、より早期の対応が可能である。
【００９７】４.システム管理者が信用できない場合
各端末とセンタの秘密鍵と公開鍵を作成するシステム管理者が信用できない場合には、例えば、次の文献３にあるように、複数のエージェントが、共同でセンタと端末の秘密を生成して配送する方法を用いると良い。文献３[K. Kurosawa, Y. Desmedt, "Optimum Traitor Tracing and AsymmetricScheme", Advances in Cryptology-EUROCRYPT'98, LNCS1403, pp. 145-157, Springer-Verlag, 1998.]
【００９８】５．センタ機能を各端末で動的に果たす場合
センタ機能を、ラウンドごとに異なる端末で行う場合には、各端末の公開鍵を公開簿に管理すると良い。また、この場合チェック検査履歴は各ラウンド単位で管理するものとし、ラウンドを超えた履歴管理はできない。
【００９９】６.楕円曲線暗号の利用
上記述べた排除方法は、基本的には有限体上の離散対数問題が困難である暗号系を利用している。この乗算を、楕円曲線上の加算演算に置き換えることにより、センタの計算量、通信量、端末の計算量を削減することができる。
【０１００】７．Traitor Tracing Schemeとの組合せ
ここで述べた仕組みを利用して、もし複製端末を押収することができた場合、任意の排除情報を端末に入力し、その出力を観測することにより、複製端末の端末ＩＤを特定することができる。
【０１０１】なお、上記の方法では、未チェックの端末は、排除情報から秘密鍵を用いてグループ鍵を求めるのに、ｋ回のベキ乗剰余演算が必要であった。この計算量を削減するため、別の排除情報の生成の方法としては、次の文献４にある方法を用いてもよい。文献４[N. Matsuzaki, J. Anzai, T. Matsumoto, "Light Weight Broadcast Exclusion Using Secret Sharing", ACISP 2000 Information Security and Privacy, LNCS1976, pp. 313-327, Springer-Verlag, 2000.]この方法を利用することにより、端末では２回のベキ乗剰余演算でグループ鍵を求めることができる。
【０１０２】ｍ台の鍵生成機関A_jで、それぞれ秘密鍵SS_jを生成する例を説明する。各端末T_iの秘密鍵SS_jを、以下のように決める。
$SS_j=\Sigma\lambda(i,\Lambda)\times SS_{i,j}$ (和はi∈Λについて行なう)
とする。ただし、
$SS_{i,j}=SS_j+f_{1,j}\times i+\cdots+f_{k-1,j}\times i^{k-1}\ mod\ q$
である。$f_{1,j},\cdots,f_{k-1,j}$は、(ｋ－１)個のＧＦ(ｑ)の元である。ただし、
$f_{k-1,j}\neq 0$

である。λ(i,Λ)は、
λ(i,Λ)=Π{L/(L-i)}(積はL∈Λ-{i}について行なう)
である。Λは、n台の端末およびダミーから選んだ任意のk台からなる集合である。各端末は、この条件を満たすm個の個別秘密鍵$SS_{i,j}$を秘密に保持する。個別秘密鍵$SS_{i,j}$より、
$S_i=\Sigma SS_{i,j} \bmod q$(和は$1\leqq j\leqq m$について行う)
を求め、端末秘密鍵S_iとして保持する。
【0103】センタCは、個別秘密鍵$SS_{i,j}$から、
$YY_{i,j}=g\hat{}SS_{i,j}$ (GF(p)上の演算)
を求め、さらに、
$Y_i=\Pi YY_{i,j}$ (GF(p)上の演算)(積は$1\leqq j\leqq m$について行う)
を求める。これを端末公開鍵Y_iとして保管する。
【0104】複数の秘密鍵を使う例を説明する。第1の秘密鍵をSとする。第1の秘密鍵Sと台数nより大きい素数または素数のべき数をpとする。(p-1)の約数をqとする。特定端末数(排除できる端末数)をd($1\leqq d<n-1$)とする。
【0105】各端末T_i($1\leqq i\leqq n$)は、$d\leqq k-2<n$を満たすkを決定し、
$S=\Sigma\lambda(i,\Lambda)\times S_i$(和はi∈Λについて行なう)
を満たす個別の第1の秘密鍵S_iを秘密に保持している。ただし、
$S_i=S+f_1\times i+\cdots+f_{k-1}\times i^{k-1} \bmod q$
である。$f_1,\cdots,f_{k-1}$は、(k-1)個のGF(q)の元である。ただし、
$f_{k-1}\neq 0$
である。
λ(i,Λ)=Π{L/(L-i)}(積はL∈Λ-{i}について行う)
Λは、n台の端末およびダミーから選んだ任意のk台からなる集合である。
【0106】第2の秘密鍵をUとする。Uは、
$U=\Sigma\lambda(i,\Lambda)\times U_i$(和はi∈Λについて行う)
である。各端末は、
$V_i=g\hat{}(U_i/S_i)$ (GF(p)上の演算)
を満たす個別の第2の秘密鍵V_iを秘密に保持している。ただし、
$U_i=U+e_1\times i+\cdots+e_{k-1}\times i^{k-1} \bmod q$
である。$e_1,\cdots,e_{k-1}$は、(k-1)個のGF(q)の元である。ただし、
$e_{k-1}\neq 0$
である。λ(i,Λ)は、
λ(i,Λ)=Π{L/(L-i)}(積はL∈Λ-{i}について行なう)
である。Λは、n台の端末およびダミーから選んだ任意のk台からなる集合である。
【0107】(k-1)個の第1のダミーの秘密鍵を、
$S_{n+1}=S+f_1\times(n+1)+\cdots+f_{k-1}\times(n+1)^{k-1} \bmod q$, ・・・,
$S_{n+k-1}=S+f_1\times(n+k-1)+\cdots+f_{k-1}\times(n+k-1)^{k-1} \bmod q$
により計算する。同様に、$U_{n+1}=U+e_1\times(n+1)+\cdots+e_{k-1}\times(n+1)^{k-1} \bmod q$, ・・・,
$U_{n+k-1}=U+e_1\times(n+k-1)+\cdots+e_{k-1}\times(n+k-1)^{k-1} \bmod q$
を計算する。センタCは、(S,p,q,g,S_1, ・・・, S_{n+k-1}, U_1, ・・・, U_{n+k-1})を保持する。端末T_iは、(S_i, V_i, p, q, g)を保持する。
【0108】センタCは、端末認証文の検証結果が正しくないかデータベースに重複登録があるd台の特定端末$T_{i1},\cdots,T_{id}$を排除するために、
(1)零でないGF(q)の元rを求めて、準備情報
$C1=g^r$ (GF(p)上の演算)
を計算する。
(2)d台の特定端末$T_{i1},\cdots,T_{id}$に対応した第1の秘密鍵$S_{i1},\cdots,S_{id}$と$U_{i1},\cdots,U_{id}$から、d個の排除サブ情報
$C3_1=r\times S_{i1}+U_{i1} \bmod q$, ・・・,
$C3_d=r\times S_{id}+U_{id} \bmod q$
を計算する。
(3)ダミーの秘密鍵$S_{n+1},\cdots,S_{n+k-1}$と$U_{n+1},\cdots,U_{n+k-1}$から任意に(k-d-1)個ずつ選んで、これらを$S_{id+1},\cdots,S_{ik-1}$, $U_{id+1},\cdots,U_{ik-1}$として、以下の(k-d-1)個の排除サブ情報
$C3_{d+1}=r\times S_{i,d+1}+U_{i,d+1} \bmod q$ ・・・,
$C3_{k-1}=r\times S_{i,k-1}+U_{i,k-1} \bmod q$
を計算する。特定端末のID番号$i_1,\cdots,i_d$と、ダミーのID番号$i_{d+1},\cdots,i_{k-1}$と、準備情報C1と、(k-1)個の排除サブ情報$C3_1,\cdots,C3_{k-1}$を、排除情報として求めて、複数台の端末に同報通信する。
【0109】センタCは、
$K=g\hat{}(r\times S+U)$ (GF(p)上の演算)
をグループ鍵として求める。正しい端末T_jが、排除情報から秘密鍵S_jとV_jを用いてグループ鍵を求める際は、
$\Lambda=\{j,i_1,\cdots,i_{k-1}\}$
とし、$\lambda(j,\Lambda),\lambda(i_1,\Lambda),\cdots,\lambda(i_{k-1},\Lambda)$を求める。準備情報C1と排除サブ情報$C3_1,\cdots,C3_{k-1}$と自身の秘密情報$S_j$と$V_j$を用いて、
$W1=S_j\times\lambda(j,\Lambda)$
$W2=C3_1\times\lambda(i_1,\Lambda)+\ldots+C3_{k-1}\times\lambda(i_{k-1},\Lambda) \bmod q$
$K=(C1\times V_j)\hat{}W1\times g\hat{}W2$ (GF(p)上の演算)
を計算する。この結果のKをグループ鍵とする。
【0110】上記のように、本発明の実施の形態では、複製端末発見方法を、センタと複数台の端末が、個々のグループ鍵で暗号通信する通信網により接続された通信

システムにおいて、センタが各端末に新規グループ鍵を配布する際に、端末で発生した乱数が複製困難なことを利用して端末IDの重複を検査することで複製端末を発見する構成としたので、複製端末の存在を自動的に検出して排除できる。また、未チェックの端末には、正規端末と不正端末を排除した排除情報を同報通信網で送信する。このため、不正端末を発見した段階で、すぐに他の未チェックの端末を含めて、新しいグループ鍵を共有できて、これを用いた暗号通信を再開することができる。

【0111】

【発明の効果】以上の説明から明らかなように、本発明では、センタと複数台の端末を含むグループ同報通信システムの複製端末発見方法を、センタは、センタ乱数を生成し、グループ鍵の更新通知とセンタ乱数をチャレンジとして同報通信を用いて複数台の端末に送信し、チャレンジを受信した端末は、ラウンドごとに端末乱数を生成し、センタ乱数と端末乱数に対する端末認証文を端末秘密鍵により生成し、端末認証文と端末乱数とをセンタ公開鍵で暗号化して端末暗号文としてセンタに送信し、センタは、グループ鍵を生成し、センタ秘密鍵で端末暗号文を復号して端末認証文と端末乱数とを得て、端末公開鍵（センタが端末の秘密鍵を管理している場合は秘密鍵）で端末認証文を検証し、端末乱数と、端末の端末ＩＤとを、対応させて登録したデータベースを検索して、同一端末ＩＤでかつ異なる端末乱数が登録されている重複登録の有無を検査し、端末認証文の検証結果が正しく、かつ重複登録が無い前記端末（正規端末と称する）の端末乱数と端末ＩＤをデータベースに登録し、この正規端末の端末乱数を用いて、グループ鍵を暗号化してセンタ暗号文として正規端末に送信し、端末認証文の検証結果が正しくないか、重複登録がある端末（不正端末と称する）と正規端末とを排除してグループ鍵を共有するための排除情報を求めて、排除情報を同報通信で送信し、正規端末は、センタ暗号文を受信し、端末乱数を用いてこれを復号してグループ鍵を得て、正規端末と不正端末以外のその他端末の端末は、センタから排除情報を受信し、端末の秘密鍵を用いてグループ鍵を得て、不正端末は、センタ暗号文あるいは排除情報を用いても、グループ鍵を得ることができずにグループ同報通信から排除される構成としたので、センタは自動的に複製端末の存在を検知でき、発見を恐れて複製端末が乱数を送らない場合には、複製端末は秘密情報を入手できないので無効化することができるという効果が得られる。

【0112】また、複製端末が発見されたときには、センタは、その端末を排除してグループ鍵を配布するための排除情報を同報通信する。これにより、未チェックの端末も正しい端末を同じグループ鍵を獲得できるため、新しいグループ鍵を用いた暗号文を早急に再開することができる。

【図面の簡単な説明】

【図１】本発明の実施の形態における複製端末発見方法の概念図、

【図２】本発明の実施の形態における複製端末発見方法で使用するセンタの構成図、

【図３】本発明の実施の形態における複製端末発見方法で使用する端末の構成図、

【図４】本発明の実施の形態における複製端末発見方法の複製端末発見フェーズ（フェーズ＃１）の流れ図、

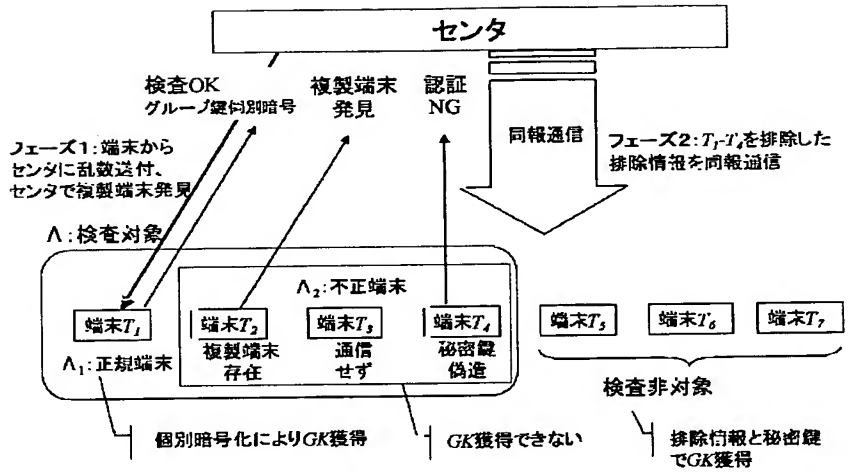
【図５】本発明の実施の形態における複製端末発見方法のグループ鍵配送フェーズ（フェーズ＃２－Ａ）の流れ図、

【図６】本発明の実施の形態における複製端末発見方法のグループ鍵配送フェーズ（フェーズ＃２－Ｂ）の流れ図である。

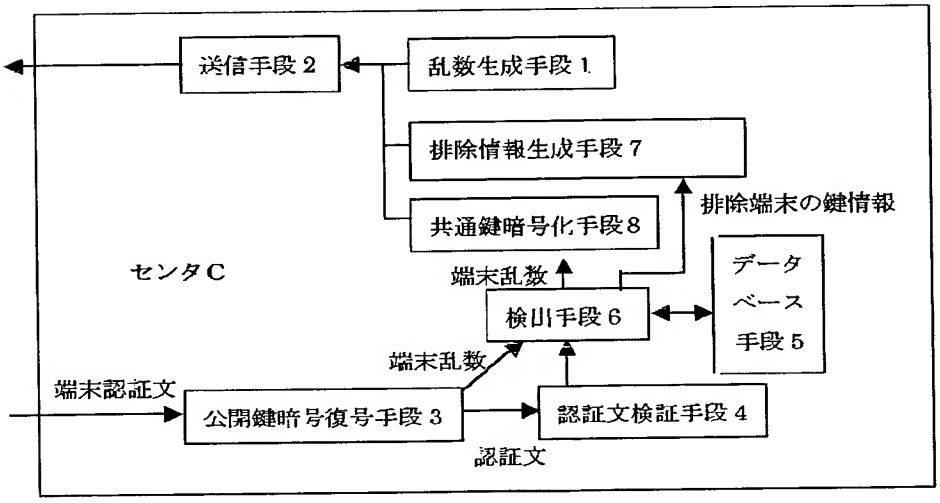
【符号の説明】

1　センタ側の乱数生成手段
2　センタ側の送信手段
3　公開鍵暗号復号手段
4　認証文検証手段
5　データベース手段
6　検出手段
7　排除情報生成手段
8　共通鍵暗号化手段
11　端末側の乱数生成手段
12　端末側の送信手段
13　第１のグループ鍵計算手段
14　認証文生成手段
15　公開鍵暗号手段
16　第２のグループ鍵計算手段
17　秘密鍵

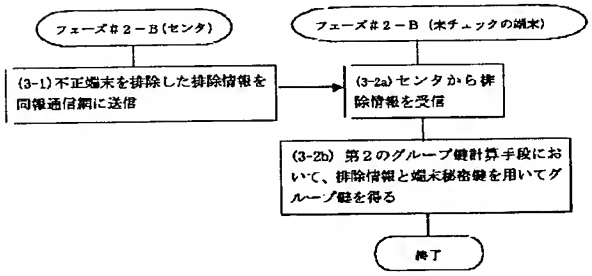
【図１】


センタ
検査OK
グループ鍵個別暗号
複製端末
発見
認証
NG
同報通信
フェーズ2：T_1-T_4を排除した
排除情報を同報通信
フェーズ1：端末から
センタに乱数送付、
センタで複製端末発見
Λ：検査対象
Λ_2：不正端末
端末T_1
端末T_2
端末T_3
端末T_4
端末T_5
端末T_6
端末T_7
Λ_1：正規端末
複製端末
存在
通信
せず
秘密鍵
偽造
検査非対象
個別暗号化によりGK獲得
GK獲得できない
排除情報と秘密鍵
でGK獲得

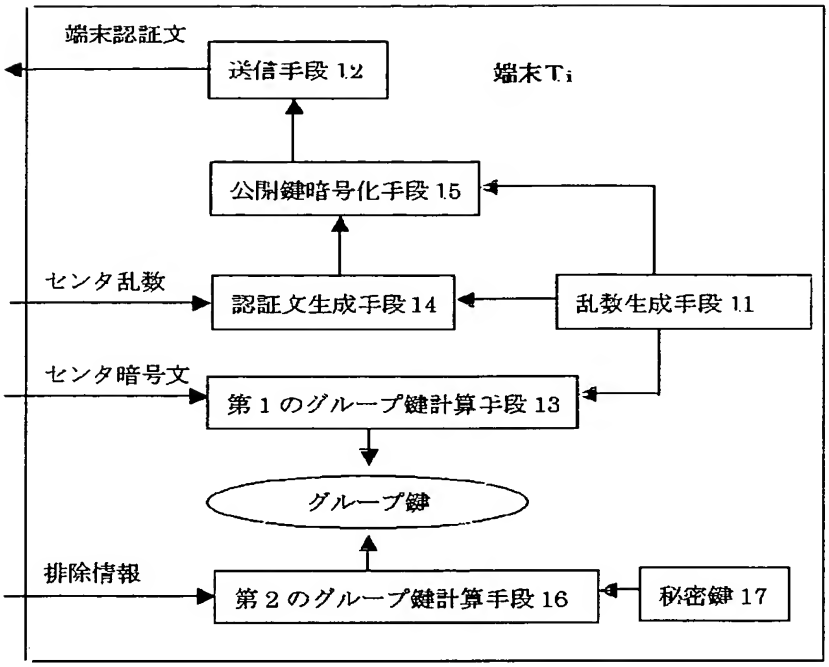
【図２】


送信手段２
乱数生成手段１
排除情報生成手段７
共通鍵暗号化手段８
排除端末の鍵情報
センタC
端末乱数
検出手段６
データ
ベース
手段５
端末乱数
端末認証文
公開鍵暗号復号手段３
認証文検証手段４
認証文

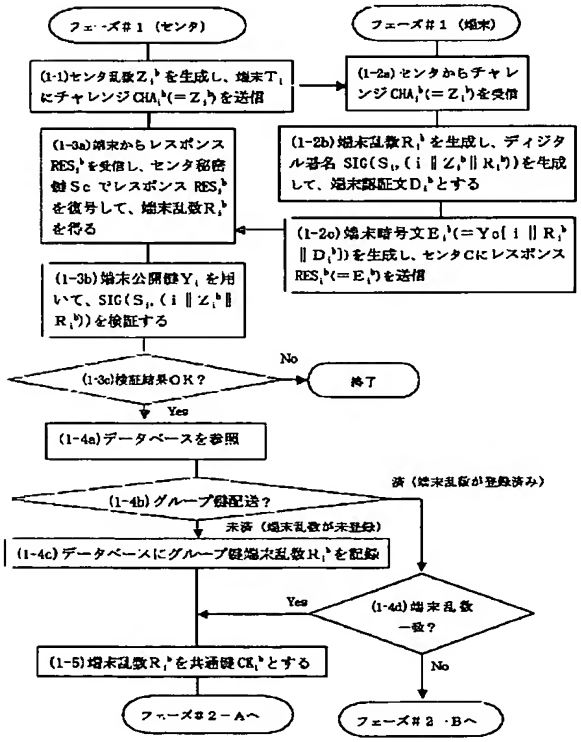
【図６】


フェーズ#２−B(センタ)
フェーズ#２−B（ICチップの端末）
(3-1)不正端末を排除した排除情報を同報通信網に送信
(3-2a)センタから排除情報を受信
(3-2b) 第２のグループ鍵計算手段において、排除情報と端末秘密鍵を用いてグループ鍵を得る
終了

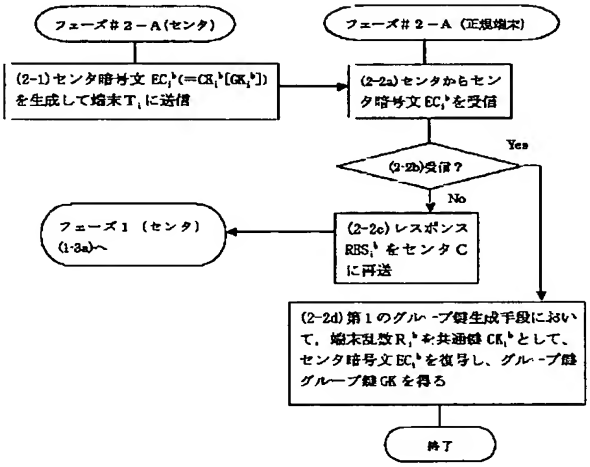
【図３】


端末認証文
送信手段 12
端末Ti
公開鍵暗号化手段 15
センタ乱数
認証文生成手段 14
乱数生成手段 11
センタ暗号文
第１のグループ鍵計算手段 13
グループ鍵
排除情報
第２のグループ鍵計算手段 16
秘密鍵 17

【図４】


フェーズ＃１（センタ）
フェーズ＃１（端末）
(1-1)センタ乱数Z_i^b を生成し、端末T_i にチャレンジCHA_i^b(=Z_i^b)を送信
(1-2a)センタからチャレンジCHA_i^b(=Z_i^b)を受信
(1-3a)端末からレスポンスRES_i^b を受信し、センタ秘密鍵Sc でレスポンスRES_i^b を復号して、端末乱数R_i^b を得る
(1-2b)端末乱数R_i^b を生成し、ディジタル署名SIG(S_i,(i‖Z_i^b‖R_i^b))を生成して、端末認証文D_i^b とする
(1-2c)端末暗号文E_i^b(=Yo[i‖R_i^b‖D_i^b])を生成し、センタCにレスポンスRES_i^b(=E_i^b)を送信
(1-3b)端末公開鍵Y_i を用いて、SIG(S_i,(i‖Z_i^b‖R_i^b))を検証する
(1-3c)検証結果OK？
No
終了
Yes
(1-4a)データベースを参照
(1-4b)グループ鍵配送？
済（端末乱数が登録済み）
未済（端末乱数が未登録）
(1-4c)データベースにグループ鍵端末乱数R_i^b を記録
(1-4d)端末乱数一致？
Yes
No
(1-5)端末乱数R_i^b を共通鍵CK_i^b とする
フェーズ＃２－Aへ
フェーズ＃２－Bへ

【図５】


フェーズ＃２－A（センタ）
フェーズ＃２－A（正規端末）
(2-1)センタ暗号文EC_i^b(=CK_i^b[GK_i^b])を生成して端末T_i に送信
(2-2a)センタからセンタ暗号文EC_i^b を受信
(2-2b)受信？
Yes
No
フェーズ１（センタ）(1-3a)へ
(2-2c)レスポンスRES_i^b をセンタCに再送
(2-2d)第１のグループ鍵生成手段において、端末乱数R_i^b を共通鍵CK_i^b として、センタ暗号文EC_i^b を復号し、グループ鍵GK を得る
終了

フロントページの続き

(72)発明者　安齋　潤
神奈川県横浜市港北区新横浜三丁目20番８号　株式会社高度移動通信セキュリティ技術研究所内

(72)発明者　松本　勉
神奈川県横浜市青葉区柿の木台13－45

Ｆターム(参考)　5J104 AA08 AA09 AA16 BA03 EA04 EA06 EA19 LA01 LA06 NA02 NA12